Index to Volume 3

ADAMS, C.: The Structured Design of Cryptographically Good S-Boxes 27
AGNEW, G. B.: An Implementation for a Fast Public-Key Cryptosystem 63
BERSON, T. A.: Guest Editors' Introduction 61
DE SOETE, M.: New Bounds and Constructions for Authentication/Secrecy Codes with Splitting 173
GAARDER, K.: Applying a Formal Analysis Technique to the CCITT X.509 Strong Two-Way Authentication Protocol 81
GODLEWSKI, P.: Key-Minimal Cryptosystems for Unconditional Secrecy 1
GOLIĆ, J. DJ.: A Generalized Correlation Attack on a Class of Stream Ciphers Based on the Levenshtein Distance 201
HABER, S.: How To Time-Stamp a Digital Document 99
KALISKI, B. S., JR.: One-Way Permutations on Elliptic Curves 187
LENSTRA, H. W., JR.: On the Chor–Rivest Knapsack Cryptosystem 149
MATYAS, S. M.: Key Processing with Control Vectors 113
MERKLE, R. C.: A Fast Software One-Way Hash Function 43
MICALI, S.: Efficient, Perfect Polynomial Random Number Generators 157
MIHALJEVIĆ, M. J.: *see* GOLIĆ, J. DJ. 201
MITCHELL, C.: *see* GODLEWSKI, P. 1
MULLIN, R. C.: *see* AGNEW, G. B. 63
ONYSZCHUK, I. M.: *see* AGNEW, G. B. 63
PASTOR, J.: CRYPTOPOST™—A Cryptographic Application to Mail Processing 137
RUEPPEL, R. A.: *see* BERSON, T. A. 61
SCHNORR, C. P.: *see* MICALI, S. 157
SNEKKENES, E.: *see* GAARDER, K. 81
STORNETTA, W. S.: *see* HABER, S. 99
TAVARES, S.: *see* ADAMS, C. 27
VANSTONE, S. A.: *see* AGNEW, G. B. 63